Docket No. 12-15184

IN THE

UNITED STATES COURT OF APPEALS

ELEVENTH CIRCUIT

MICHAEL BERGER, Petitioner/Appellant, v. UNITED STATES OF AMERICA, Respondent/Appellee.	28 U.S.C. § 2255 Appeal Northern District of Florida Lower Case Nos: 3:09-cv-551-LC-EMT 3:08-cr-22-LC-EMT-1

RENEWED APPLICATION FOR A CERTIFICATE OF APPEALABILITY

MICHAEL UFFERMAN
Michael Ufferman Law Firm, P.A.
2022-1 Raymond Diehl Road
Tallahassee, Florida 32308
(850) 386-2345/fax (850) 224-2340
FL Bar No. 114227
Email: ufferman@uffermanlaw.com

Counsel for Petitioner/Appellant **BERGER**

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

The following certificate of interested persons and corporate disclosure statement is provided pursuant to Federal Rule of Appellate Procedure 26.1 and Eleventh Circuit Rule 26.1-1:

Berger, Michael; Petitioner/Appellant

Collier, Lacey A.; Senior District Judge, United States District Court, Northern District of Florida

Goldberg, David L.; Assistant United States Attorney, Northern District of Florida

Hendrix, Michelle Lynn; Previous counsel for Michael Berger

Marsh, Pamela C.; United States Attorney, Northern District of Florida

Sprowls, Paul Alan; Assistant United States Attorney, Northern District of Florida

Timothy, Elizabeth M.; Magistrate Judge, United States District Court, Northern District of Florida

Ufferman, Michael; Counsel for Michael Berger

The Petitioner/Appellant, MICHAEL BERGER, by and through undersigned counsel and pursuant to 28 U.S.C. § 2253(c)(2) and Eleventh Circuit Rule 22-1, moves the Court to issue a certificate of appealability (COA) authorizing the appeal of the denial of his motion filed pursuant to 28 U.S.C. § 2255. As explained below, the issue in this case is whether defense counsel rendered ineffective assistance of counsel by failing to file a motion to suppress the evidence illegally seized from Mr. Berger's residence (evidence that was obtained pursuant to a search warrant affidavit that omitted material facts). Notably, the search warrant affidavit alleged that law enforcement officials believed that Mr. Berger had been using the Internet to access child pornography, but the affidavit *failed* to mention that a records custodian had informed law enforcement officials – prior to the date that the affidavit was prepared – that Mr. Berger's Internet account had been compromised. Mr. Berger submits that "reasonable jurists could debate" this issue and therefore it is appropriate to grant a COA in this case.

A. Statement of the Facts.

1. Procedural History.

Mr. Berger was convicted (following the entry of a guilty plea) in the United States District Court, Northern District of Florida, of one count of knowingly receiving child pornography in interstate and foreign commerce via the computer, in violation of 18 U.S.C. § 2252A(a)(2). Mr. Berger was sentenced to 180 months'

imprisonment. Mr. Berger timely filed a motion pursuant to 28 U.S.C. § 2255. (Doc 839).[1] The magistrate judge subsequently entered a report and recommendation recommending that the motion be denied. (Doc 899). Notably, in the report and recommendation, the magistrate judge did "not disagree that information about Defendant's account having been compromised . . . would have been relevant to the reviewing judge." (Doc 899 - Pg 16). The district court adopted the magistrate judge's report and recommendation and denied the § 2255 motion. (Doc 910).

B. Standard for issuance of a COA.

In *Miller-El v. Cockrell*, 537 U.S. 322, 336, 123 S. Ct. 1029, 1039 (2003), the Supreme Court held that a COA should be issued if a petitioner can show that "reasonable jurists could debate whether (or, for that matter, agree that) the petition should have been resolved in a different manner or that the issues presented were adequate to deserve encouragement to proceed further." The Supreme Court explained:

> This threshold inquiry does not require full consideration of the factual or legal bases adduced in support of the claims. In fact, the statute forbids it. When a court of appeals side steps this process by first deciding the merits of an appeal, and then justifying its denial of a COA based on its adjudication of the actual merits, it is in essence deciding an appeal without jurisdiction.
>
> To that end, our opinion in *Slack* [*v. McDaniel*, 529 U.S. 473, 120

[1] Citations to the documents referenced in this pleading will be to the documents filed in case number 3:08-cr-22-LC-EMT-1.

> S. Ct. 1595 (2000),] held that a COA does not require a showing that the appeal will succeed. Accordingly, a court of appeals should not decline the application for a COA merely because it believes the applicant will not demonstrate an entitlement to relief. The holding in *Slack* would mean very little if appellate review were denied because the prisoner did not convince a judge, or, for that matter, three judges, that he or she would prevail. It is consistent with § 2253 that a COA will issue in some instances where there is no certainty of ultimate relief. After all, when a COA is sought, the whole premise is that the prisoner "has already failed in that endeavor." *Barefoot* [*v. Estelle*, 463 U.S. 880,] 893 n.4[, 103 S. Ct. 3383, 3395 n.4 (1983)].

Id. at 336-37, 123 S. Ct. at 1039. The Supreme Court defined the test for issuing a COA as follows:

> We do not require petitioner to prove, before the issuance of a COA, that some jurists would grant the petition for habeas corpus. Indeed, a claim can be debatable even though every jurist of reason might agree, after the COA has been granted and the case has received full consideration, that petitioner will not prevail. As we stated in *Slack*, "[w]here a district court has rejected the constitutional claims on the merits, the showing required to satisfy § 2253(c) is straightforward: *The petitioner must demonstrate that reasonable jurists would find the district court's assessment of the constitutional claims debatable or wrong."* 529 U.S. at 484[, 120 S. Ct. at 1595].

Id. at 338, 123 S. Ct. at 1040 (emphasis added). As explained below, Mr. Berger submits that reasonable jurists would find the magistrate judge's/district court's assessment of his § 2255 motion debatable.

C. Mr. Berger's § 2255 claim: defense counsel rendered ineffective assistance of counsel by failing to file a motion to suppress the evidence illegally seized from Mr. Berger's residence (evidence which was obtained pursuant to a search warrant affidavit that omitted material facts).

In his § 2255 motion, Mr. Berger alleged that defense counsel rendered

ineffective assistance of counsel by failing to file a motion to suppress the evidence illegally seized from his residence (evidence that was obtained pursuant to a search warrant affidavit that omitted material facts). On February 27, 2008, the Government filed an "Affidavit in Support of a Search Warrant" in the United States District Court for the Eastern Division of Virginia (Richmond Division). The affidavit sought a search warrant in order to search Mr. Berger's residence. The affidavit stated the following regarding the alleged "probable cause" that was the basis for seeking the search warrant:

> 17. During June 2006, representatives from the Queensland Police Service, Brisbane, Australia, informed members of the FBI's Innocent Images unit of an international child pornography investigation regarding numerous subjects residing in various countries. Investigation to date indicates that a number of individuals (i.e., members) participating in this enterprise are located in the United States. The investigation involves a sophisticated and extremely organized group, hereafter referred to as "enterprise," of Internet Usenet users involved in the prolific trade/distribution of child pornography. The enterprise employs highly technical and advanced security measures to avoid law enforcement detection. Such techniques include, but are not limited to, the use of Pretty Good Privacy (PGP) software to encrypt messages posted to the enterprise's pre-designated newsgroup location where members communicate with each other, PGP encryption of binary files (which generally contain child pornographic material) uploaded to other newsgroup locations, and the swapping of file extensions which subsequently must be re-swapped in order to successfully download a particular picture or movie file.
>
> 18. This investigation is predicated on information obtained from an individual who has been charged criminally in an unrelated child pornography investigation. This individual informed law enforcement that he/she was a member of this enterprise and identified a newsgroup titled "alt.anonymous.message" as the location at that time

where members of the enterprise conducted/uploaded text [message] postings to communicate with each other. It is noted that since the time that the above referenced information was provided by the cooperating individual, the newsgroup location has changed several times. At this particular newsgroup location, members inform each other as to the newsgroup location (i.e. a different location) of where they have uploaded child pornography for members to go to download for their own personal collections. The child pornography binary files, either still pictures or video files, are never uploaded (i.e. distribution/transportation) to the newsgroup reserved for text [message] communications between members. Rather, the child pornography is uploaded to other innocuous newsgroup locations where members must go to retrieve/download the material. Specific directions are posted in the enterprise's newsgroup location, such as passwords, to ensure the successful retrieval/download of the image and/or video files.

19. The subject of the aforementioned investigation provided investigators with his/her PGP encryption keys which have allowed law enforcement to access, decrypt and monitor all activity/postings associated with the enterprise. Basically, law enforcement has infiltrated the enterprise. To date, investigators have collected extremely valuable and incriminating evidence from various members of the enterprise. Since the initial monitoring of the newsgroups, approximately 403,442 images and 1,128 video files have been advertised, distributed and/or received by the enterprise (period of 08/31/2006 through 12/15/2007).

20. The enterprise currently consists of approximately 45 active members. There is a defined hierarchy or structure to the enterprise and all members must abide by strictly enforced written security measures and standard operating procedures in order to retain their membership status. To become a member of the enterprise, one must be invited in by an existing member, he/she must be known to trade child pornography material (i.e. demonstrated by being involved in other newsgroups involved in this activity), and must pass a timed written test to determine their knowledge of child pornographic material (*e.g.,* knowledge of the names of various child pornography series; must be able to describe a particular series in question, etc.). The test also serves as a measure to access whether the interested party could be an undercover law enforcement officer attempting to infiltrate the enterprise. Members of the enterprise are told never to provide their true identities to another

member of the enterprise. They are never to communicate with one another using traditional email, chat, Yahoo, ICQ or telephone. For the security of the enterprise as a whole, their relationship with other members of the enterprise is limited strictly to contacts via the Internet. In this manner, if one of the members of the enterprise is ever arrested by law enforcement, that member cannot provide any identifying information to law enforcement on other members of the enterprise.

21. The enterprise has developed outside contacts in the child pornography industry whereby they have made specific requests for the production of new child pornography material. In several instances, it appears the enterprise has been able to order new (unreleased) child pornography movies produced solely for the benefit of the enterprise (*i.e.* material which had not been distributed to the public in other child pornography forums). In addition, the enterprise has established an E-gold account, funded by the members, in order to purchase newly released child pornography material from various international producers.

22. As indicated above, the enterprise periodically moves from one newsgroup location to another where they each member provided conduct their primary text [chat] message communications with each other [sic]. This is done primarily for two reasons: 1) as a general principle to avoid law enforcement detection, and/or 2) because someone in the group made a mistake, violating the enterprise's written security procedures (*e.g.,* failure to encrypt a message/posting, thus making it readily available for anyone to access and read), which would jeopardize the security of the group. Each time the enterprise moves from one newsgroup location to another, they also change all of their PGP encryption keys so there is no trail from one newsgroup location to the next location. Additionally, each time the enterprise moves, all of the members change their nicknames. For the most part, the selection of new nicknames is based on a particular theme that the leader of the group established for all of the members to use/follow. For example, during one of the enterprise moves from one newsgroup location to another, the group adopted a theme related to cars (motor vehicles). As such, each of the members created a new nickname based on this theme *(e.g.* Thunderbird, Jaguar, Fender, Big Block, etc.) During a recent move from one newsgroup location to the current newsgroup location, all PGP encryption keys and nicknames changed; however, it was decided the theme would revert back to the previously used "Japanese"

theme.

Significantly, law enforcement has identified a group user, originally nicknamed Yardbird, who apparently play the role of group leader or moderator for the enterprise. Investigators have determined that every time the group changes forums, Yardbird previously received from each user his new nickname/moniker and new personal PGP keys. Each users new personal PGP key must be encrypted using the prior (or current) personal PGP key, which therefore provides a direct link and digital fingerprint. Upon receiving the new nicknames and personal PGP keys, Yardbird distributed to the group a list of new nicknames that included a reference to the most recent previous nickname. Investigators monitoring the group were able to work backwards and link each nickname and associated personal PGP key with the prior nickname and personal PGP key.

. . . .

SPECIFIC SUBJECT LOCATION INFORMATION

23. Michael D. Berger has been identified as a subject of this investigation. As further described below, he is directly associated with the following nicknames used by him to communicate with other members of the child exploitation enterprise: "Box of Rocks," "Safrane," "Artery-Clogger," "Cartman," "Suslik," "Hanako" and "Volsch."

24. On September 2, 2006, an individual utilizing the nickname "artery-clogger" (a.k.a Michael Berger) accessed the newsgroup located at alt.anonymous.message and posted the following message with message-ID <44f9b233$33399$bb4e3ad8@newscene.com> and with subject line "Mushroom Puffs:"[2]

. . . .

29. On May 17, 2007 at 8:36 AM, administrative subpoena IINI 1975 was served on Newscene Usenet News service, P.O. Box xxxxx, Omaha, NE 68145-xxxx. The subpoena requested subscriber information for the individual responsible for the post on September 10,

---

[2] The affidavit stated that the files accessed on September 2, 2006, contained images of child pornography. The affidavit further stated that an individual using Mr. Berger's Newscene Usenet Service account accessed child pornography on other dates (September 10, 2006, September 23, 2006, July 27, 2007, August 5, 2007, and September 13, 2007).

2006, with the message identification <45049638$0$33463$bb4e3ad8@newscene.com>

30. On May 30, 2007, a response was received for administrative subpoena IINI 1975 from Novia Corp. (d/b/a Newscene Usenet News Service), which contained the following subscriber information:

Account Name:	saxwork
Real Name:	Mike Berger
Email Address	saxwork@comcast.net
Customer since:	May 1, 2000 - present

. . . .

42. On August 3, 2007 at 8:16 AM, administrative subpoena IINI 2312 was served on Newscene Usenet Service, P.O. Box xxxxx, Omaha, NE 68145-xxxx. The subpoena requested all account history, including but not limited to, changes to the account (i.e. payment method, name, etc.) login information and if/where available activity logs/history for any account in the name of Michael Berger or being paid for by debit card number xxxxxxxxxxx8534 or with an address of xxxxx Drawbridge Court, Mechanicsville, VA 23116.

43. On August 14, 2007, a response was received for administrative subpoena IINI 2312, from Newscene, which contained IP login data, billing logs and requests for changes to Mr. Berger's account. The following is a summary of the information provided:

Account Name:	saxwork
Real Name:	Mike Berger
Email Address:	saxwork@comcast.bet
Customer since:	May 1, 2000 - present
Credit Cards used	xxxxxxxxxxxx6774
	xxxxxxxxxxxx1105
	xxxxxxxxxxxx9519
	xxxxxxxxxxxx5434
E-mail addresses used:	saxwork@attbi.com
	Grommik@aol.com
	saxwork@comcast.net
IP logs:	January 2, 2007 to August 14, 2007

. . . .

69. Based on the foregoing information , there is probable cause to believe that Michael D. Berger, a/k/a "Box of Rocks," "Safrane." "Artery-Clogger," "Cartman." "Suslik," "Hanako" and

> "Volsch," and residing at xxxxx Drawbridge Court, Mechanicsville, VA 23116, advertised and distributed child pornography via the Internet as part of a child exploitation enterprise.

In his § 2255 motion, Mr. Berger explained that material information was omitted from the affidavit and the omitted information undermines the probable cause determination in this case.

Notably, in September of 2006, the Government issued a subpoena to the Newscene Usenet News Service (hereinafter "Newscene") requesting information relating to the Newscene account that allegedly accessed child pornography files on September 2, 2006 (Subpoena IINI 1048). On September 15, 2006, Michael S. McMahon, a records custodian with Newscene, sent an email to the Government stating the following:

> As we discussed briefly in our conversation on 9/13/06, the message cited in the subpoena *was posted through an account that was compromised*. The only information I am able to confirm with certainty is the IP address from which the message was posted and the time at which the connection to our server was initiated and terminated . . . .

(Emphasis added). The documents attached to Mr. McMahon's September 15, 2006, email indicate that the post in question came from an IP address originating in Nurenberg, Germany. Later that year, the Government issued a second subpoena to Newscene requesting information relating to the Newscene account that allegedly accessed child pornography files on September 10, 2006 (Subpoena IINI 1275). On

January 3, 2007, Mr. McMahon sent a letter to the Government stating the following:

> The message with Message-ID <45049638$0$33463$bb4e3ad8@newscene.com> was posted using the same account involved in IINI 1048 (issued 9/11/06). As we discussed at that time, *the account was compromised*.

(Emphasis added). The documents attached to Mr. McMahon's January 3, 2007, letter indicate that the post in question came from an IP address originating in Middletown, New Jersey.

Notably, the Government's affidavit for a search warrant *completely fails* to mention that the Newscene records custodian had informed the Government that Mr. Berger's Newscene account had been compromised.[3]

Mr. Berger retained an Information Technology (IT) expert (Michael L. Meacham) to review his case (and in particular, to review and advise regarding what it meant when Mr. McMahon stated that Mr. Berger's account had been "compromised"). Mr. Meacham opined the following regarding Mr. Berger's compromised account:

- Although there are a series of posts to the account owned by Mr. Berger, the dates of the posts are not supported by the IP addresses used in the subpoena. In other words, anyone using Mr. Berger's username and

[3] Mr. Berger further notes that his Newscene account continued to be accessed *after* he was arrested (clearly demonstrating that someone other than Mr. Berger was accessing this account). (Doc 498 - Pg 15).

password could have made those posts. The Government stated in the subpoena that the header of a post might only contain the username. The Government further stated that no one in the "enterprise" knew who anyone else was. Hence, it is impossible to tie a nickname to an actual person. The two crucial pieces of evidence missing are the IP addresses used to make the offending posts and that Mr. Berger actually knew and used the nicknames.[4]

- The Government gave a list of IP addresses tied back to Mr. Berger and a list of dates used. NONE of these date appear to have been when the Government says the offending material was posted.
- It is entirely possible that a group of people used the nicknames in question (i.e., "artery-clogger") and that an accomplice could search the newsgroup for postings by an individual using this name.
- The search warrant affidavit makes much of tracing the IP addresses used by Mr. Berger to Comcast, but none of these postings occurred on a date when objectionable material was posted. The Government did not

[4] An example of this is the Government's assertion that Mr. Berger utilized the nickname "artery-clogger" and posted a message on September 2, 2006, titled "Mushroom Puffs" that contained objectionable material. Yet, Mr. McMahon's September 15, 2006, email and the documents attached to that email establish that this account had been compromised and that this posting came from an IP address originating in Nurenberg, Germany.

include the IP addresses used with the objectionable postings.

Mr. Meacham's report was attached to Mr. Berger's § 2255 pleadings. (Doc 840).

Based on the foregoing, Mr. Berger asserted in his § 2255 motion that had the Government's affidavit for a search warrant included the fact that Mr. Berger's account had been compromised, there would not have been sufficient probable cause to issue a search warrant. Under *Franks v. Delaware*, 438 U.S. 154, 155-56, 98 S. Ct. 2674, 2676 (1978), if a

> defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request. In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false materials set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

The *Franks* rationale applies to material that has been deliberately or recklessly omitted from a search warrant affidavit. *See United States v. Reivich*, 793 F.2d 957, 960 (8th Cir. 1986). In *Reivich*, the court held that the defendant "had to show (1) that the police omitted facts with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading, . . . and (2) that the affidavit if supplemented by the omitted information would not have been sufficient to support

a finding of probable cause." *Id.* at 961 (citations omitted).

In the instant case, Mr. Berger is able to satisfy both prongs set forth in *Reivich*. First, the Government omitted facts with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading. The affidavit completely fails to mention that Mr. McMahon informed the Government that Mr. Berger's Newscene account had been compromised and that the account was being accessed by IP addresses *all over the world*. The affidavit was filed on February 27, 2008. Mr. McMahon informed the Government of the compromised account in 2006 (and again in 2007). The only conclusion that can be reached from the failure to include the "compromised account" information in the affidavit is that either the Government intentionally misled the court or the Government acted with reckless disregard of the truth. Any reasonable person would have known that this was the kind of information the judge would wish to know. Second, the affidavit – if supplemented by the omitted information – would not have been sufficient to support a finding of probable cause in this case. The entire basis for probable cause in this case was that Mr. Berger's Newscene account was being utilized to view/post illegal content. If the court had been informed that Mr. Berger's account had been compromised (and that the account was being accessed by IP addresses all over the world), then there would have been insufficient facts to support a finding of probable cause to justify the search of Mr. Berger's residence.

In support of his argument, Mr. Berger relies on *United States v. Jacobs*, 986 F.2d 1231 (8th Cir. 1993). In *Jacobs*, a law enforcement officer obtained a search warrant to search a package (and subsequently a residence) based on a suspicion of illegal drug possession. In the affidavit for the search warrant, the officer claimed that a narcotics dog "showed interest" in the package, but the officer omitted that the dog had failed to alert to drugs in the package. In addition, the magistrate judge was not notified that a second canine sniff of the same package was negative. The Eighth Circuit held that if the warrant application was reworked to include the omitted information, such an application would not support probable cause:

> The defendant's argument that the police violated *Franks* by omitting key information from the warrant application is more forceful. First, he argues that by omitting "Turbo's" failure to alert, Officer Brotherton was deliberately misleading the magistrate judge. Secondly, the defendant argues that the failure to notify Brotherton and the magistrate judge that the second canine sniff was negative further violated *Franks* by depriving the magistrate judge of key information necessary to a determination of probable cause.
>
> Officer Brotherton correctly informed the magistrate judge that the dog had shown an interest in the Jacobs package, but neglected to include Henderson's statement that no alert had occurred. In order for this omission to be a violation of *Franks* and *Reivich*, the defendant must make two showings. The first is a showing that the police omitted the information with the intent to make, or in reckless disregard of whether they made, the affidavit misleading. *Reivich*, 793 F.2d at 961; *United States v. Lueth*, 807 F.2d 719, 726 (8th Cir. 1986). In the present case, "Turbo's" failure to alert was omitted from the affidavit. Because of the highly relevant nature of the omitted information, we hold the omission occurred at least with reckless disregard of its effect upon the affidavit. Brotherton knew that the dog had failed to alert to the box before he submitted the affidavit to the magistrate judge, yet he did not

include this information. Any reasonable person would have known that this was the kind of thing the judge would wish to know.

Under *Reivich*, the failure to include the information and a reckless disregard for its consequences may be inferred from the fact that the information was omitted. However, in order for this inference to be valid, the defendant must show that the omitted material would be "'clearly critical' to the finding of probable cause." 793 F.2d at 961 (quoting *United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980)). The omission of the fact that the dog failed to alert to the package satisfies this criterion.

Having shown that relevant information was recklessly omitted from the warrant application, Jacobs must further show that the affidavit, if supplemented with the omitted information, would not be sufficient to support a finding of probable cause. *Reivich*, 793 F.2d at 961; *Lueth*, 807 F.2d at 727. "[O]nly if the affidavit as supplemented by the omitted material could not have supported the existence of probable cause" will suppression be warranted. *Lueth*, 807 F.2d at 726.

In this case, if the warrant application were reworked to include the omitted phrase, it would read something like this: "The dog had showed an interest in the [defendant's] package, but had not given a full alert to the package." Testimony of Detective Henderson, Suppression Hearing Tr. 39. We hold that such an application, on its face, would not support probable cause. The evidence in support of probable cause would be limited to the information that Officer Brotherton received from Officer Billingsley in Phoenix, plus the fact that the dog had shown an interest in the package, but had not alerted to it. Without an alert, the police clearly lacked the probable cause necessary to open the package. While the information received from Officer Billingsley, plus the fact that the dog showed an interest in the package, might have provided reasonable suspicion that it contained contraband, more is needed to overcome the defendant's Fourth Amendment right to privacy in its contents. In this case, the failure to inform the magistrate judge that the dog had not given its trained response when confronted with a package containing drugs, coupled with the dog handler's admission that he could not say with certainty that drugs were in the package, causes us to hold that the warrant would not have been supported by probable cause, if the omitted material had been included.

Jacobs, 986 F.2d at 1234-35. Pursuant to *Jacobs*, if the affidavit in the instant case

was reworked to include the omitted information, the affidavit would not support probable cause. The reworked affidavit would read as follows: "an account registered to Mr. Berger has accessed illegal material on the Internet but we have learned that the account has been compromised and has been used by people all over the world." This information would have been insufficient under the Fourth Amendment to justify a search of Mr. Berger's residence.[5]

After Mr. Berger was charged in this case, he informed defense counsel that his account had been compromised. All of the information contained in this pleading regarding the subpoenas and Mr. McMahon's responses to the pleadings was available to defense counsel. Yet, defense counsel failed to advise Mr. Berger that he should/could file a motion to suppress the evidence seized in this case. Had defense counsel filed a motion to suppress, Mr. Berger submits that the motion would

---

[5] It is important to note that after Mr. Berger was charged, the Government acknowledged that he was not the person who it originally thought he was when the affidavit was prepared. Notably, at the rearraignment hearing, the Government stated:

> Also, from here on in, the government would request that any documents or nomenclature revolving around the defendant strike the a/k/a, Box Of Rocks, and just refer to the defendant as Michael Berger.
>
> And these discussions revolved around what the government deems to be a legal and ethical obligation. *This defendant is completely and utterly distinguishable from the rest of the defendants who have been indicted in this case . . . .*

(Doc 492 - Pg 3) (emphasis added).

have been granted and the evidence seized during the search of Mr. Berger's residence would have been suppressed. *See Wong Sun v. United States*, 371 U.S. 471, 484-85, 83 S. Ct. 407, 415 (1963) (stating that evidence found during an unlawful search should be suppressed as the fruit of the poisonous tree). Had the evidence been suppressed in this case, the case would have been dismissed (i.e., absent the evidence seized as a result of the unlawful search of Mr. Berger's residence, there was no basis for the charges in this case). As a result, Mr. Berger was denied his right to effective assistance of counsel in violation of the Sixth Amendment to the Constitution. But for counsel's ineffectiveness, the result of the proceeding would have been different. *See Hill v. Lockhart*, 474 U.S. 52, 57, 106 S. Ct. 366, 369-70 (1985).

In the report and recommendation, the magistrate judge did "not disagree that information about Defendant's account having been compromised . . . would have been relevant to the reviewing judge." (Doc 899 - Pg 16). Yet, the magistrate judge denies relief for two reasons: (1) a recently prepared affidavit by an FBI agent (Barbara Cordero) claiming that Mr. Berger's account was not compromised[6] and (2) the magistrate judge's conclusion that probable cause still would have been

[6] Ms. Cordero asserted that Mr. Berger was involved in the use of TOR" – "a network of virtual tunnels . . . that act as a three chain anonymous encrypted proxy" – which in Ms. Cordero's opinion made it appear as if Mr. Berger's account was compromised. (Doc 899 - Pg 13 n. 10).

established even if the "omitted" fact of the compromised account had been disclosed in the search warrant affidavit.

Regarding Ms. Cordero's affidavit, Mr. Berger submits that the magistrate judge erred by relying on a recently prepared document – a document that contains information that was *not disclosed* in the original search warrant affidavit. The sufficiency of the evidence supporting probable cause is limited to the information presented in the four corners of the affidavit. *See United States v. Laughton*, 409 F.3d 744, 751 (6th Cir. 2005). Hence, reliance by the Government and the magistrate judge on TOR is improper – because the Government failed to include such a TOR allegation in the search warrant affidavit. Moreover, both parties have submitted affidavits from witnesses who have offered opinions concerning whether Mr. Berger's account was compromised: the Government submitted an affidavit from Ms. Cordero and Mr. Berger submitted a report and an affidavit from Information Technology expert Michael L. Meacham who opined that "[t]he evidence clearly shows that an internet account under the control of Michael Berger was compromised (hacked) allowing access to his account from persons located worldwide." (Doc 840-6 - Pg 3). However, despite these conflicting opinions, the magistrate judge seemingly made a credibility determination and relied on Ms. Cordero's opinion – and the magistrate judge did this *without holding an evidentiary hearing*. As the Fourth Circuit recognized in *United States v. Stokes*, 112 Fed. Appx. 905, 906 (4th

Cir. 2004), "[w]hen the issue is one of credibility, resolution on the basis of affidavits can rarely be conclusive." The Fourth Circuit added "we find that the conflicting statements in the affidavits submitted by Stokes and counsel create a factual dispute requiring an evidentiary hearing." *Id. See also Daniels v. United States,* 54 F.3d 290, 293 (7th Cir. 1995) (granting evidentiary hearing on § 2255 petition based on conflicting evidence contained in sworn affidavits). Thus, it was error for the magistrate judge to recommend that Mr. Berger's petition be denied on the basis of Ms. Cordero's affidavit without first holding an evidentiary hearing.

Regarding the magistrate judge's conclusion that probable cause still would have been established even if the "omitted" fact of the compromised account had been disclosed in the search warrant affidavit, the magistrate judge reaches this conclusion by relying on several cases. (Doc 899 - Pgs 14-16). Mr. Berger submits that the cases cited by the magistrate judge are distinguishable from the instant case because, unlike the instant case, *none of the cases cited by the magistrate judge involve a situation where Government agents knew that an account had been compromised prior to seeking a search warrant and yet failed to include this information in the affidavit in support of the search warrant*.

In its response to Mr. Berger's § 2255 motion, the Government did not dispute that it was informed by Mr. McMahon that Mr. Berger's account had been

compromised. Hence, it is unrefuted that the Government omitted a material fact from the affidavit (as found by the magistrate judge). The issue then becomes whether the search warrant affidavit – if supplemented by the omitted information – would have been sufficient to support a finding of probable cause in this case. Mr. Berger submits that the omitted facts negate probable cause. The entire basis for probable cause in this case was that Mr. Berger's Internet account was being utilized to view/post illegal content. *If the court had been informed that Mr. Berger's account had been compromised (i.e., someone else was logging into the account using Mr. Berger's username and password and that the account was being accessed by IP addresses all over the world), then there would have been insufficient facts to support a finding of probable cause to justify the search of Mr. Berger's residence*. *See Jacobs*, 986 F.2d 1231.

D. Conclusion.

Mr. Berger submits that he has satisfied the test set forth in *Miller-El* for the issuance of a COA (i.e., reasonable jurists can debate whether the § 2255 motion should have been resolved in a different manner or that the issue presented is adequate to deserve encouragement to proceed further). Accordingly, Mr. Berger requests the Court to issue a COA in this case.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY a true and correct copy of the foregoing instrument has been furnished to:

Office of the United States Attorney
21 East Garden Street, Suite 400
Pensacola, Florida 32502-2593

by U.S. mail this 8th day of November, 2012.

Respectfully submitted,

/s/ Michael Ufferman
MICHAEL UFFERMAN
Michael Ufferman Law Firm, P.A.
2022-1 Raymond Diehl Road
Tallahassee, Florida 32308
(850) 386-2345/fax (850) 224-2340
FL Bar No. 114227
Email: ufferman@uffermanlaw.com

Counsel for Petitioner/Appellant **BERGER**